The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
08/26/2020

SUBJECT:
Multiple Vulnerabilities in Mozilla Firefox Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Mozilla Firefox and Mozilla Firefox ESR, the most severe of which could allow for arbitrary code execution. Mozilla Firefox is a web browser used to access the Internet. Mozilla Firefox ESR is a version of the web browser intended to be deployed in large organizations. Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution in the context of the logged-on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Mozilla Firefox versions prior to 80
- Mozilla Firefox ESR versions prior to 68.12 and 78.2

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Mozilla Firefox and Firefox Extended Support Release (ESR), the most severe of which could allow for arbitrary code execution. Details of the vulnerabilities are as follows:

- A lock was missing when accessing a data structure and importing certificate information into the trust database. (CVE-2020-15668)
- By holding a reference to the eval() function from an about:blank window, a malicious webpage could have gained access to the InstallTrigger object which would allow them to prompt the user to install an extension. Combined with user confusion, this could result in an unintended or malicious extension being installed. (CVE-2020-15664)
- During ECDSA signature generation, padding applied in the nonce designed to ensure constant-time scalar multiplication was removed, resulting in variable-time execution dependent on secret data. (CVE-2020-12401)
- A vulnerability exists which shows evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. (CVE-2020-15670)
- Firefox did not reset the address bar after the before unload dialog was shown if the user chose to remain on the page. This could have resulted in an incorrect URL being shown when used in conjunction with other unexpected browser behaviors. (CVE-2020-15665)
- If Firefox is installed to a user-writable directory, the Mozilla Maintenance Service would execute updater.exe from the install location with administrative privileges. Although the Mozilla Maintenance Service does ensure that updater.exe is signed by Mozilla, the version could have been rolled back to a previous version which would have allowed exploitation of an older bug and arbitrary code execution with system privileges. Note: This issue only affected Windows operating systems. Other operating systems are unaffected. (CVE-2020-15663)
- When aborting an operation, such as a fetch, an abort signal may be deleted while alerting the objects to be notified. This results in a use-after-free and we presume that with enough effort it could have been exploited to run arbitrary code. (CVE-2020-15669)
- When converting coordinates from projective to affine, the modular inversion was not performed in constant time, resulting in a possible timing-based side channel attack. (CVE-2020-12400)
- When performing EC scalar point multiplication, the wNAF point multiplication algorithm was used; which leaked partial information about the nonce used during signature generation. Given an electro-magnetic trace of a few signature generations, the private key could have been computed. (CVE-2020-6829)
- When processing a MAR update file, after the signature has been validated, an invalid name length could result in a heap overflow, leading to memory corruption and potentially arbitrary code execution. Within Firefox as released by Mozilla, this issue is only exploitable with the Mozilla-controlled signing key. (CVE-2020-15667)
- When trying to load a non-video in an audio/video context the exact status code (200, 302, 404, 500, 412, 403, etc.) was disclosed via the MediaError Message. This level of information leakage is inconsistent with the standardized onerror/onsuccess disclosure and can lead to inferring login status to services or device discovery on a local network among other attacks. (CVE-2020-15666)

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution in the context of the logged-on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate updates provided by Mozilla to vulnerable systems, immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Mozilla:
https://www.mozilla.org/en-US/security/advisories/mfsa2020-36/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-37/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-38/

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12400
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12401
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15663
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15664
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15665
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15666
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15667
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15668
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15669
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15670
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6829